BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

Pengiriman data/pesan dari suatu tempat ke tempat lain menggunakan media teknologi banyak terkendala dengan permasalahan keamanan. Oleh karena itu kebutuhan keamanan semakin meningkat jika data/pesan tersebut mengandung pesan rahasia, sehingga tidak sembarang orang boleh membacanya. Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, fungsi dari teknik steganografi yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas. Steganografi membutuhkan dua properti, yaitu pesan dan media penampung. Salah satu media penampung yang digunakan dalam pengiriman pesan adalah dengan menumpangkannya ke sebuah citra digital. Karena citra digital tersusun dari *pixel* yang terdiri dari kolom dan baris, melalui *pixel* inilah suatu citra dapat dimanipulasi untuk menyimpan informasi yang akan digunakan sebagai salah satu pengimplementasian teknik steganografi.

Untuk menghasilkan steganografi yang baik tanpa menimbulkan kecurigaan maka dibutuhkan beberapa kriteria yaitu data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra (*Robustness*), data yang disembunyikan harus dapat diungkapkan kembali (*Recovery*), dan *Fidelity* yaitu setelah disisipi dengan teks/pesan, media penampung harus tetap terlihat baik. Jika pesan disisipkan kedalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Steganografi pada media digital file gambar digunakan untuk mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan

rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna pada file gambar yang telah disisipi pesan rahasia. Dengan keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra digital yang telah disisipi pesan rahasia. Metode *Bit Plane Complexity Segmentation* (BPCS) merupakan metode yang diperkenalkan oleh Eiji Kawaguchi dan O.Eason pada tahun 1998. Metode BPCS memanfaatkan perhitungan kompleksitas pada tiap *bit-plane*.

Pada penelitian yang dilakukan oleh Anggraini dan Ema Utami [8] pada tahun 2007 penyisipan pesan pada citra menggunakan metode BPCS hanya pada satu format citra saja yaitu bitmap. Oleh karena itu pada tugas akhir ini akan diteliti lebih lanjut dengan menggunakan format citra selain bitmap yaitu citra format PNG. Format PNG digunakan karena penyimpanan citra menggunakan teknik kompresi *lossless* yaitu tidak menghilangkan bagian dari citra tersebut ketika dikompresi. Format PNG mendukung jenis pewarnaan RGB sehingga tidak akan memiliki masalah besar dilihat dari aspek perubahan sebelum dan sesudah disisipi pesan [11].

Jika hanya mengandalkan teknik steganografi saja data tidak dapat terjaga, karena dapat menjadi celah dari sisi keamanan. Banyak aplikasi *steganalysis* digunakan untuk mendeteksi data pesan yang terdapat di dalam citra stego. Oleh karena itu, kriptografi bermanfaat sebagai pengaman untuk data pesan sehingga data pesan tidak bisa langsung dibaca ketika sudah diambil dari citra stego karena berupa kode-kode yang tidak bisa dimengerti.

Berdasarkan uraian latar belakang yang telah dijelaskan, penulis ingin membuat aplikasi dan mengetahui tingkat keamanan dan kelebihan menggunakan metode BPCS sehingga penulis mengangkat judul **“PEMBANGUNAN APLIKASI STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN METODE *BIT PLANE COMPLEXITY SEGMENTATION* (BPCS) DAN ALGORITMA XTEA UNTUK KEAMANAN DATA”**

1.2. Identifikasi Masalah

Berdasarkan dari penjelasan yang sudah diuraikan dalam latar belakang, maka dapat diperoleh identifikasi masalah mengenai bagaimana membangun aplikasi steganografi menggunakan metode *Bit Plane Complexity Segmentation* (BPCS) untuk menyembunyikan pesan rahasia dan dapat meningkatkan keamanan data menggunakan kriptografi dengan algoritma XTEA.

1.3. Maksud dan Tujuan

Maksud dari penulisan tugas akhir ini adalah membangun aplikasi steganografi pada citra digital menggunakan metode *Bit Plane Complexity Segmentation* (BPCS) dan algoritma XTEA untuk keamanan data.

Sedangkan tujuan yang ingin dicapai adalah :

1. Mengimplementasikan penyembunyian pesan atau informasi kedalam citra digital menggunakan metode *Bit Plane Complexity Segmentation* (BPCS) dan algoritma XTEA.
2. Melakukan pengujian terhadap keamanan pesan menggunakan aplikasi *steganalysis* yaitu *StegSpy2.1*.
3. Untuk mengetahui besar pesan yang dapat disembunyikan ke dalam citra menggunakan metode *Bit Plane Complexity Segmentation* (BPCS).
4. Untuk mengetahui kualitas citra yang telah disisipi pesan pada metode *Bit Plane Complexity Segmentation* (BPCS) dengan menggunakan metode *Peak Signal-to-Noise Ratio* (PSNR).
5. Melakukan pengujian ketahanan pesan terhadap manipulasi pada citra yang telah disisipi pesan yaitu dengan cara merotasi dan memotong citra yang telah disisipi pesan.

1.4. Batasan Masalah

Batasan masalah bertujuan untuk memudahkan perancangan dan menghindari meluasnya permasalahan, maka batasan masalahnya yaitu :

1. Metode steganografi menggunakan metode *Bit Plane Complexity Segmentation* (BPCS)
2. Media penampung pesan yang digunakan hanya berupa citra yang memiliki format *.bmp, dan *.png
3. Pesan yang dapat disembunyikan hanya berupa file teks yaitu *.txt.
4. Metode enkripsi menggunakan metode XTEA dengan algoritma enkripsi simetris yaitu algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi.
5. Panjang kunci algoritma XTEA 128 bit untuk enkripsi pesan yang akan disisipkan kedalam citra.
6. Nilai batas/*threshold* yang digunakan pada metode BPCS yaitu 0.3. Nilai batas/*threshold* digunakan untuk mencari *bit-plane* yang tergolong *informative region* atau *noise-like region*.
7. Hal – hal yang akan diujikan pada aplikasi yang dibangun yaitu :
   a. Keamanan pesan terhadap aplikasi *steganalysis* yaitu menggunakan *StegSpy 2.1*
   b. Besar pesan yang dapat disisipkan ke dalam citra
   c. Kualitas citra yang telah disisipi pesan yang dinyatakan dalam PSNR
   d. Ketahanan citra yang telah disisipi pesan dengan cara merotasi citra-stego, dan memotong citra-stego menggunakan *Adobe Photoshop.*
8. Pembangunan aplikasi menggunakan metode berorientasi objek dan pemodelannya menggunakan UML.
9. Aplikasi yang dibangun akan digunakan pada sistem operasi berbasis desktop.
10. Tools yang digunakan dalam pembuatan aplikasi steganografi dengan menggunakan Java Netbeans 6.8.

1.5. Metode Penelitian

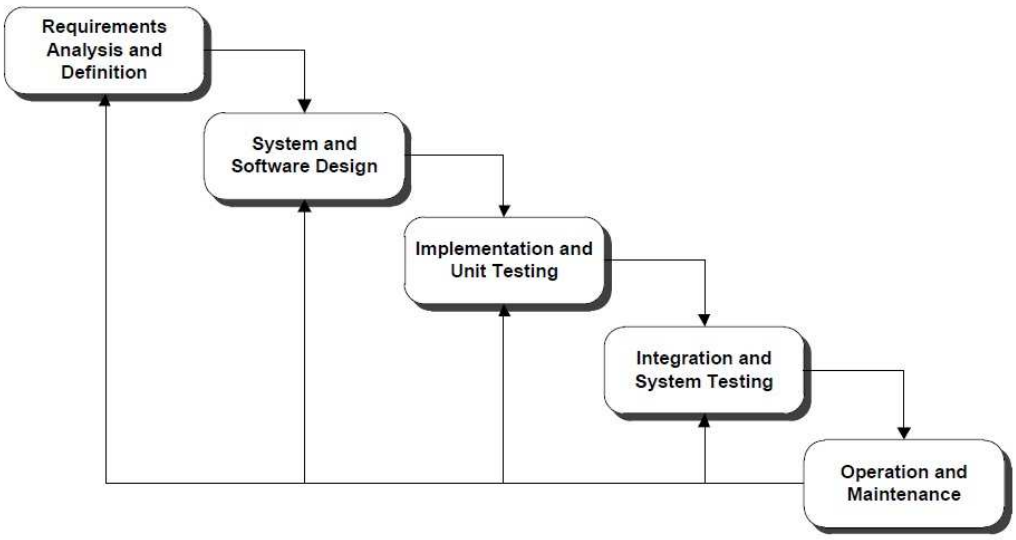
Metodologi penelitian yang digunakan dalam penulisan skripsi ini menggunakan metode analisis deskriptif yang terdiri dari dua metode yaitu metode pengumpulan data, dan metode pembangunan perangkat lunak.

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah menggunakan metode studi literatur. Studi literatur merupakan pengumpulan data dengan cara mengumpulkan literature, jurnal ilmiah, situs-situs di internet, *paper* dan bacaan-bacaan yang ada kaitannya dengan judul penelitian. Pada tahap ini akan dilakukan pengumpulan data dari literatur dan pustaka mengenai steganografi pada citra digital, metode *Bit Plane Complexity Segmentation* (BPCS) dan algoritma XTEA

1.5.2 Metode Pembangunan Perangkat Lunak.

Metode pembuatan perangkat lunak menggunakan paradigma perangkat lunak secara *waterfall*, yang meliputi beberapa proses. Berikut ini akan dijelaskan mengenai tahap-tahap pembangunan sistem dengan menggunakan paradigma *waterfall* seperti pada gambar 1.1.



Gambar 1.1 Metode *Waterfall*

Tahapan-tahapan dari model *waterfall* ini adalah sebagai berikut:

1. *Requirements Analysis and Definition*

   Tahap ini merupakan bagian dari kegiatan aplikasi yang terbesar dalam pengerjaan suatu proyek. Pada tahap ini dilakukan analisa terhadap permasalahan dan menetapkan berbagai kebutuhan yang diperlukan dalam pembangunan atau pengembangan suatu perangkat lunak.

   Dimulai dari analisis masalah untuk menentukan kebutuhan aplikasi, melakukan analisis pada proses pengkonversian secara manual dan mengubahnya ke dalam serangkaian algoritma, pemilihan model yang tepat untuk pemodelan aplikasi hingga pendefinisian *class* dan tipe data

2. *System and Software Design*

   Tahap menerjemahkan kebutuhan-kebutuhan yang dianalisis ke dalam bentuk yang mudah dimengerti. Sehingga didapat jelas fungsi dan kebutuhan yang diinginkan dari pembangunan atau pengembangan perangkat lunak penyisipan pesan kedalam citra menggunakan metode *Bit Plane Complexity Segmentation* (BPCS), sebelumnya pesan dienkripsi menggunakan algoritma XTEA untuk menambah keamanan data. Langkah selanjutnya yang dilakukan adalah merancang tampilan perangkat lunak agar mudah dimengerti oleh pengguna sesuai dengan fungsi dan kebutuhan perangkat lunak steganografi menggunakan metode BPCS.

3. *Implementation and unit testing*

   Tahap penerjemahan data atau pemecahan masalah yang telah dirancang kedalam suatu bahasa pemrograman tertentu. Sehingga dihasilkan sebuah perangkat lunak steganografi menggunakan metode BPCS yang sesuai dengan kebutuhan pengguna. Setiap fungsional yang ada pada perangkat lunak dilakukan uji kelayakan, sehingga perangkat lunak steganografi menggunakan metode BPCS dapat berjalan dengan baik.

4. *Integration and System Testing*

   Pada tahap ini, dilakukan penyempurnaan terhadap perangkat lunak steganografi menggunakan metode BPCS secara keseluruhan agar dapat berjalan sesuai dengan kebutuhan. Pengujian perangkat lunak dilakukan dengan membandingkan pesan yang disembunyikan pada beberapa format citra. Sehingga bisa diketahui format citra apa yang bagus dan baik sebagai media penampung menggunakan metode BPCS.

5. *Operation and Maintenance*

   Tahap akhir dimana perangkat lunak steganografi menggunakan metode BPCS yang sudah selesai dapat dioperasikan langsung oleh pengguna. Tahap *maintenance* perlu dilakukan untuk disesuaikan apabila ada perubahan sesuai dengan permintaan pengguna.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini menguraikan tentang latar belakang permasalahan, identifikasi inti permasalahan yang dihadapi, menentukan maksud dan tujuan penelitian, yang kemudian diikuti dengan pembatasan masalah, metode penelitian, serta sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah pernah dilakukan sebelumnya termasuk sintesisnya.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas mengenai sub-sub sistem yang diuraikan dari sistem utama dengan tujuan untuk mengetahui cara kerja dan interaksi dari tiap sub

sistem dalam fungsinya untuk mencapai tujuan sistem. Didalamnya terdapat analisis terhadap proses pembangkit kunci, proses enkripsi, proses penyisipan, proses ekstraksi, dan proses dekripsi selain itu terdapat juga kebutuhan fungsional dan nonfungsional dari sistem, perancangan antarmuka untuk aplikasi yang akan dibangun sesuai dengan hasil analisis yang telah dibuat.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini membahas tentang implementasi dari aplikasi yang dibangun. Implementasi dilakukan berdasarkan analisis dan perancangan yang telah dilakukan, kedalam bahasa pemrograman tertentu. Hasil dari implementasi, kemudian dilakukan pengujian apakah aplikasi telah sesuai seperti yang diharapkan.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan berdasarkan hasil penelitian yang telah dilakukan dan masukan-masukan yang dapat digunakan untuk pengembangan perangkat lunak selanjutnya.